



# National Infrastructure Protection Center NIPC Daily Open Source Report for 23 January 2003

Current Nationwide  
Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- Alabama News Channel 19 reports there has been a threat to poison the water supply in Columbus, Mississippi and residents are urged to drink bottled water while the threat is being investigated. (See item [20](#))
- CERT has released Vulnerability Note VU#650937: CVS server improperly deallocates memory, which says that a "double-free" vulnerability in the Concurrent Versions System (CVS) server could allow an unauthenticated, remote attacker with read-only access to execute arbitrary code, alter program operation, read sensitive information, or cause a denial of service. (See item [30](#))
- Microsoft has released Security Bulletin MS03-003: Flaw in how Outlook 2002 handles V1 Exchange Server Security Certificates, which could lead to information disclosure. (See item [31](#))
- Microsoft has released Security Bulletin MS03-001: Unchecked buffer in Locator service could lead to code execution. (See item [32](#))
- Microsoft has released Security Bulletin MS03-002: Cross-Site Scripting flaw in Microsoft Content Management Server 2001 (See item [33](#))

### **NIPC Update Fast Jump**

**Production Industries:** [Energy](#); [Chemical](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [General](#); [NIPC Web Information](#)

## **Energy Sector**

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 22, Associated Press* — **Corrosion found in TVA nuclear reactor. Leaking reactor coolant caused minor corrosion to a reactor at the Tennessee Valley Authority's (TVA) Sequoyah nuclear power plant (Tennessee) but was never a safety problem, a Nuclear Regulatory Commission (NRC) spokesperson said. It was the second case of boric acid corrosion in the nuclear power industry since more severe damage was reported in March 2001 at the Davis-Besse plant in Ohio.** The damage at the Sequoyah plant's Unit 2 reactor was discovered following an unrelated shutdown on Dec. 26, according to an NRC notice. "It is just some residue with slight corrosion, but they did find it and they didn't find any evidence of serious problems elsewhere," Ken Clark, an Atlanta region spokesperson for the NRC, said Tuesday. **TVA spokesperson John Moulton said the corrosion at the Sequoyah plant near Soddy-Daisy caused a "slight indentation on the reactor vessel head that did not require repair."** Moulton said in addition, "The NRC was notified, but there was no threat to the health and safety of employees and the public." He said the leak was repaired and the reactor was returned to service. **TVA operates six nuclear reactors in Tennessee and Alabama as part of a system that provides electricity to 8.3 million people in Tennessee and parts of Kentucky, Virginia, North Carolina, Alabama, Georgia and Mississippi.**  
Source: [http://www.austin360.com/aas/news/ap/ap\\_story.html/National/AP.V0369.AP-Reactors-Corros.html](http://www.austin360.com/aas/news/ap/ap_story.html/National/AP.V0369.AP-Reactors-Corros.html)
2. *January 22, BBC Monitoring* — **The Kozloduy nuclear power plant's third reactor will be connected to the country's grid in three days.** This is what Kozloduy nuclear power plant Executive Director Kostadinov has told Khorizont Radio. Our reporter Iva Antonova has more: [Antonova] **The repairs started last night after the necessary measures had been taken yesterday in accordance with technological instructions, Kostadinov said. I recall that the third reactor was shut down yesterday morning because of a mechanical defect in the protection system.** The protection system was activated as a result of decreased pressure in the first circuit and a leak of water during technological operations. There are no changes in the radiation background. According to the preliminary assessment, the event is classified at level zero of the seven-level Exchange of Nuclear Information Scale and does not have an impact on the reactor's safety.  
Source: [http://www.energycentral.com/sections/newsroom/nr\\_article.cfm?id=3587491](http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3587491)
3. *January 21, PRNewswire* — **The U.S. energy crisis: an urgent request for action. The Industrial Energy Consumers of America (IECA) and thirty one diverse organizations have sent a letter to Congress, key Administration officials, and state Governors urging them to take action to stem the national energy crisis.** Some high points are as follows. **The high cost of natural gas is having a devastating impact on manufacturing competitiveness and jobs.** U.S. natural gas production has been stagnant since 1995 even though we have an abundant resource base and prices that is double their historical base. **The manufacturing sector has lost 2 million jobs since 1998 and energy costs are a major contributing factor.** It is particularly critical that Congress and the states act to increase supply of natural gas; and address regulations, such as New Source Review, in a manner that makes it easier for power generators to meet air quality standards without switching from coal to natural gas. Congress must also expedite commercialization of clean coal technology, the ultimate solution for power generation using coal in an environmentally acceptable manner. Leadership is needed by the U.S. Congress and the states to put our country on the road to an affordable and reliable energy supply. **The Industrial Energy Consumers of America (IECA) is a nonprofit organization**

of manufacturers for which the availability, use and cost of energy, power or hydrocarbon feedstock play a significant role in their ability to compete in domestic and world markets.

Source: [http://www.energycentral.com/sections/gasnews/gn\\_article.cfm?id=3582487](http://www.energycentral.com/sections/gasnews/gn_article.cfm?id=3582487)

[[Return to top](#)]

## **Chemical Sector**

4. *January 21, Business Report* — **Three plants face growing economic problems in a troubled sector. After a year that saw a handful of plants either sell or fold, three more Louisiana companies have released information in recent weeks outlining additional layoffs or closures.** On Jan. 8, SeaRiver Marine Inc. announced immediate plans to close its Baton Rouge office, which handles marine transport for Exxon/Mobil. On New Year's Day, Vulcan Chemicals began accepting "voluntary separations" from salaried employees in an effort to soften the impact of potential layoffs. And following a Nov. 5 Business Report story detailing layoffs at Triad Nitrogen in Donaldsonville, the company informed employees in December that more terminations are expected by late this month. Jim Richardson, professor of economics at Louisiana State University, says **three things are working against the industry: the high value of the U.S. dollar, which makes American products more expensive around the world; rising natural gas prices; and stiffer international competition.** Tim Ryan, dean of the business school at the University of New Orleans, adds a number of other concerns, including the fact that technology may be making part of the workforce obsolete. "The chemical industry in Louisiana is part of the world economy. The U.S. as well as the world economies aren't growing as fast as everyone expected. Also, many chemical companies have been going through technology upgrades. And they do it in such a way that they are labor-saving devices," Ryan said.

Source: [http://www.businessreport.com/pub/21\\_10/industry/3107-1.html](http://www.businessreport.com/pub/21_10/industry/3107-1.html)

[[Return to top](#)]

## **Defense Industrial Base Sector**

5. *January 22, Washington Post* — **More civilians accompanying U.S. military. In military hot spots around the world, civilians are performing duties once reserved for military personnel — building barracks, running kitchens, maintaining tanks and jets, and even helping to plan strategy.** During the Persian Gulf War, some units had one contractor for 50 military personnel while others had one for every 25, according to research by Peter W. Singer, a fellow at the Brookings Institution. In the Balkans, there was one contractor per 10 soldiers, Singer said. The ratio of contractors to combatants could increase even more if the United States goes to war in Iraq, he said. **The Defense Department does not keep track of the number of contractors overseas but recognizes that such assignments are part of a growing trend, said spokesman Glenn Flood. The General Accounting Office reported that 10 percent of the \$13.8 billion spent on Balkans operations from 1995 through March 2000 went to private companies.** Private-sector companies have played a part in military operations overseas for decades, but their numbers grew in the 1990s. And as the military deploys complex weapons systems faster, contractors go overseas to provide training that there

wasn't time for in the United States. "Starting after 1991, you had the combination of the military being forced to downsize and this real push to privatize anything and everything," said Singer of the Brookings Institution. "The problem is that it's been fairly random." Along with contracting out logistical or support tasks such as feeding military personnel or mowing lawns, the military has also handed over to companies some duties that straddle the line between contractor and soldier, such as maintaining tactical systems and drone aircraft, Singer said. There are essentially no rules for how contractors should behave in a war zone, and there is no effort within the industry to create any, according to industry analysts. The contractors don't have to follow the military codes of conduct. Contractors are usually not allowed to carry weapons but could be expected to pick up arms if they are attacked, industry officials said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A24741-2003Jan21.ht ml>

6. *January 22, Associated Press* — **Pentagon calls up largest number of guard and reservist since start of terror war.** More than 20,000 National Guard and reserve forces reported for active duty this week as the U.S. Defense Department continued its buildup for a possible war with Iraq. **It was the biggest one-week jump in mobilizations for overseas or domestic duty since the Sept. 11, 2001, terrorist attacks.** Gen. Richard Myers, chairman of the Joint Chiefs of Staff, told reporters that more reserves will be called but that the number would not rise dramatically unless President George W. Bush decides to go to war to topple Iraqi President Saddam Hussein. **Under an order signed by President Bush three days after the 2001 terrorist attacks, up to 1 million guard and reserve forces can be called to serve for up to two years. But Myers said that if war is averted the mobilization total would not exceed 100,000.**

Source: [http://story.news.yahoo.com/news?tmpl=storyp\\_won\\_po/na\\_gen\\_us\\_reserves\\_activated\\_3](http://story.news.yahoo.com/news?tmpl=storyp_won_po/na_gen_us_reserves_activated_3)

7. *January 20, Washington Post* — **Many layers to building a super soldier.** Imagine a futuristic battleground where soldier uniforms as light as paper resist bullets, treat wounds, and detect chemical and biological poisons, where soft fabrics morph into splints, and battle suit sensors relay details about a soldier's location and physical condition to headquarters. **Such is the science fiction scenario envisioned for the real 21st century world by researchers and scientists at the Institute for Soldier Nanotechnologies, one of the nation's newest Army-sponsored research centers and the largest military defense project undertaken here at the Massachusetts Institute of Technology.** The nearly \$100 million project, which also involves industry partners DuPont Co. and Raytheon Co. and two Boston hospitals, is designed to develop and apply molecular materials that will help outfit American soldiers in a way that gives them a significant edge over their enemies. It is a huge challenge, to be solved by research on the smallest scale. Now one of the hottest scientific fields, nanotechnology consists of the ability to engineer structures out of particles so tiny that hundreds could fit on the period at the end of this sentence. **Overall, the goal is to reduce uniform size and weight — a fully equipped soldier now may carry more than 100 pounds and a dozen batteries to operate different pieces of equipment — while creating a piece of clothing as self-contained as an automobile.** "You don't decide whether you need your radio or seat belt or room in your trunk. All that is built in the car when you get in," said Henry Everitt, the Army Research Office's executive manager in charge of the project. "We want the soldier to have the same luxury." **Military applications are likely to be transferred to the**

civilian and aerospace arena, participants said. Super-soldier suits could be worn by firefighters and other emergency personnel who face increasingly diverse hazards in a post-Sept. 11, 2001, world, they said. Thomas said early successes are needed to instill confidence, and some progress in detection and reactive coatings has been made. The presence of anthrax, for example, can now be detected in three minutes, instead of 24 hours.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A15185-2003Jan19.html>

8. *January 20, Aviation Week & Space Technology* — **Podded laser countermeasures seen for fighters, civil aircraft.** With the threat from shoulder-fired heat-seeking missiles against aircraft growing, Defense Department researchers are mulling the possibility of establishing a program to equip fighters and possibly even commercial airliners with a podded laser infrared countermeasures device. **The project is one of several U.S. Air Force initiatives to improve protection for aircraft operating overseas. For instance, the service this month awarded a contract for an emergency upgrade to 12 C-17 transports to give the airlifters a limited laser-based infrared self-protection capability as they fly into the Middle East as part of the buildup of U.S. forces against Iraq. Other efforts are aimed at protecting airlifters against surface-to-air missiles or aircraft and helicopters on the ground in remote locations.** The Pentagon is working on several laser infrared countermeasures systems, fielding them on helicopters and even large transports. But the current projects deliver self-protection equipment that has to be integrated into the aircraft. By using a podded configuration, "the overall cost of the system will be cut drastically," said William Taylor, who oversees the activity for the Air Force Research Laboratory's (AFRL's) sensors directorate. **While fighters are the primary applications for such a system, USAF stressed the potential civil application. Engineers note a pod would probably have enough laser energy output to protect a large airliner. Other types of infrared countermeasures devices would also be available, but Taylor noted that lasers can provide a much greater jamming energy than older technologies, such as lamp-based devices.** The Defense Department hasn't determined, yet, whether it will launch a formal program to develop the pod. AFRL, teamed with the Navy, is asking industry what options may exist for such a device, in the hope of generating interest, a formal requirement and funding. However, AFRL believes that from a technology perspective a podded electronic warfare device could be developed.

Source: <http://www.awsonline.com/cgi-bin/authenticate.pl?destination=docs/issues/20030120/aw49.htm>

[[Return to top](#)]

## **Banking and Finance Sector**

9. *January 23, Washington Post* — **The Securities and Exchange Commission voted yesterday to back away from some tough restrictions on accounting firms that it had considered in the wake of widespread corporate accounting scandals.** One of the most controversial proposals would have prohibited accounting firms from crafting tax shelters for audit clients and could have cost the firms millions of dollars in lost revenue. Investor activists saw the proposal as a bold stroke to restore public confidence, but it was strongly opposed by the accounting industry. The five commissioners – three Republicans and two Democrats appointed by President Bush – voted unanimously for a rule that would instead allow all tax services to continue. "Passing watered-down rules does nothing to restore investor confidence,"



New York State Comptroller Alan Hevesi said through a spokesman. Yesterday's vote was the most comprehensive set of accounting firm rules the SEC has adopted under an investor protection bill, known as the Sarbanes–Oxley Act, that Congress passed last summer, after financial scandals at Enron, WorldCom and other companies sent stocks plummeting. To convince investors they could trust financial reports and resume buying stocks, lawmakers said the close ties between accounting firms and their clients should be severed and other steps should be taken to force auditors to be more aggressive watchdogs.

Source: [http://www.boston.com/dailyglobe2/023/business/SEC\\_establishes\\_rules\\_for\\_accounting\\_sector+.shtml](http://www.boston.com/dailyglobe2/023/business/SEC_establishes_rules_for_accounting_sector+.shtml)

10. *January 21, Associated Press* — **Identity theft complaints double in 2002.** Complaints about identity theft nearly doubled in 2002 as the fast-growing crime topped the government's list of consumer frauds for a third consecutive year. **The Federal Trade Commission reports that 43 percent of roughly 380,000 complaints involved the hijacking of someone's identity information, such as credit card or Social Security number, to steal money or commit fraud.** The figures come from a government database of complaints collected from the FTC, the FBI and scores of law enforcement and consumer groups. Gripes about fraud in Internet auctions ranked No. 2 and accounted for 13 percent of complaints. **Outlining the most-frequent complaints on a nationally broadcast interview Wednesday, the FTC's Howard Beales said reports from consumers have increased with greater awareness of the problem prompted by recent high-profile identity-theft cases.** Up to 700,000 people in the United States may be victimized by identity bandits each year, the Justice Department says. It costs the average victim more than \$1,000 in expenses to cope with the damage to their accounts and reputations, the FTC has said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A26571-2003Jan22.html>

11. *January 17, Reuters* — **Allied Irish Banks trader gets 7.5 years for fraud.** A former currency trader for Allied Irish Banks Plc was sentenced to seven and a half years in prison on Friday for **hiding over \$691.2 million in losses at Ireland's largest bank in one of the biggest banking scandals in history.** John Rusnak, 38, whose currency portfolio had been seen as a solid performer at AIB's Baltimore-based subsidiary Allfirst Financial Inc. until last February, was also barred for life from working for any federally-insured banking institution. As part of a deal worked out with prosecutors last October, Rusnak pleaded guilty to one count of bank fraud and agreed to the punishment. **He admitting that he devised a complex five-year scheme to collect salary and bonuses totaling \$850,000 from 1997 to 2001 by hiding risky yen-dollar investments that went wrong and spun out of control.** In addition to the prison sentence he must spend five years in supervised release and pay restitution to the company or its economic successor at a rate of \$1,000 a month after he leaves jail. He also was ordered to attend drug, alcohol and gambling addiction counseling.

Source: [http://story.news.yahoo.com/news?tmpl=story&\\_nm=/crime\\_trader\\_dc\\_3](http://story.news.yahoo.com/news?tmpl=story&_nm=/crime_trader_dc_3)

12. *January 17, Comptroller of the Currency* — **Money laundering: a banker's guide to avoiding problems, December 2002.** Money-laundering methods have become more creative since the 1989 and 1993 versions of this booklet were published. **This is due to the expansion of products and services offered, more complicated financial relationships, advances in technology, and the increased velocity of money flows worldwide. Terrorist financing, although only one aspect of money laundering, has become a critical concern following the**

**events of September 11, 2001.** The Office of the Comptroller of the Currency requires regulated institutions to develop and implement effective anti-money laundering programs that encompass terrorist financing. **This has included record searches against U.S. government lists of suspected terrorists and terrorist organizations. the USA PATRIOT Act contains provisions to combat international terrorism and block terrorist access to the U.S. financial system. Several international organizations have also issued measures to curb money laundering and terrorist financing.**

Source: <http://www.occ.treas.gov/moneylaundering2002.pdf>

[\[Return to top\]](#)

## **Transportation Sector**

13. *January 22, Newsday* — **LaGuardia security director resigns. The aviation security chief at LaGuardia Airport is resigning after less than eight months on the job to run public safety at St. John's University.** Allan Hoehl, 63, said Tuesday that he will leave LaGuardia on Feb. 8, making him the first airport security director to resign since the federal government took over security screening last February. Hoehl (pronounced "Hale") took over LaGuardia security in June and oversaw the hiring of 800 government employees to check passengers and baggage, replacing the private guards who became a target of criticism after the Sept. 11 hijackings. **Hoehl said he was comfortable leaving because he had overseen the "major work" of putting the federal security screeners in place.** Most recently, LaGuardia, the nation's 22nd-largest airport with 22 million passengers in 2001, started screening all checked baggage for explosives.

Source: <http://www.newsday.com/news/local/newyork/ny-uslag223098799jan22.0.23062.story?coll=ny-nynews-reddots-headlines>

14. *January 21, Plain Dealer* — **Company proposes swipe cards to make airports safer.** A fledgling Cleveland, OH area company believes it has a fast, hassle-free way to make air travel safer than ever. **A credit-card-type approval system would be used to check dozens of databases in search of suspected terrorists, dangerous individuals and people using stolen passports or identities.** Before a passenger goes through airport security, his driver's license or other government identification is swiped through a card reader. Within seconds, security gets feedback from several databases about the person. A green light means it's OK to proceed; yellow means caution; and red is a high-alert signal, meaning security personnel could stop the passenger. Security personnel could have an answer to a question before the passenger walks through the metal detector. Federal security agents, not the company's employees, would operate the system. The system's producers have received federal approval to run a demonstration project. Mike Young, the U.S. Transportation Security Administration's director for the Cleveland, Akron-Canton and Youngstown airports, said the first test would be at Akron-Canton Regional Airport.

Source: <http://www.cleveland.com/news/plaindealer/index.ssf?/base/cuyahoga/1043145093173100.xml>

[\[Return to top\]](#)

## Postal and Shipping Sector

15. *January 22, Globe and Mail Update* — **Ottawa to boost ports' security.** Transport Minister David Collenette announced \$172.5-million in funding for marine security Wednesday, a move to improve scrutiny of vessels and people coming into Canada through marine borders and ports post Sept. 11. The Transport Minister said improving security at maritime ports will "directly benefit all Canadians through improved national security and benefit Canada's shipping industry." The funds will be directed at a number of new measures aimed at protecting Canada's marine infrastructure, improved surveillance and tracking of marine traffic. **As part of the improved tracking and surveillance system, Transport Canada will now require that all vessels be equipped with an Automatic Identification System. The system, which uses wireless and land-based communications, is able to broadcast data about a ship's identity and position along with other data.**

Source: [http://www.globeandmail.com/servlet/ArticleNews/front/RTGAM/20030122/wcoll0121\\_2/Front/homeBN/breakingnews](http://www.globeandmail.com/servlet/ArticleNews/front/RTGAM/20030122/wcoll0121_2/Front/homeBN/breakingnews)

16. *January 21, U.S. Customs Service* — **Malaysia signs Declaration of Principles to join U.S. Customs Container Security Initiative.** U.S. Customs Commissioner Robert C. Bonner and Datuk Abdul Halil Bin Abdul Mutalib, Director-General of Customs of the Government of Malaysia, announced Monday that the government of Malaysia has agreed to participate in the U.S. Customs Container Security Initiative (CSI). Director-General Datuk Abdul Halil Bin Abdul Mutalib and U.S. Customs Service Deputy Commissioner Douglas M. Browning conducted the signing ceremony on Monday, January 20 at Putrajaya, Malaysia. **Under terms of the declaration, U.S. Customs officers will be stationed at the ports of Klang and Tanjung Pelepas.** "I am very pleased that the government of Malaysia has agreed to join with the United States in the Container Security Initiative," said Commissioner Bonner. "We recognize the high volume of trade between the Ports of Klang and Tanjung Pelepas and seaports in the U.S. and Malaysia's role as an intermodal transport hub for cargo originating in many countries. This is an important step, not only for the protection of trade between the U.S. and the government of Malaysia, but for the protection of the most critical component of the world trading system as a whole – containerized cargo."

Source: <http://www.customs.ustreas.gov/hot-new/pressrel/2003/0121-01.htm>

[[Return to top](#)]

## Agriculture Sector

17. *January 22, Visalia Times-Delta* — **California creates cattle rules.** State agriculture officials are taking steps to ensure California is no longer vulnerable to bovine tuberculosis with new regulations governing the importation of dairy cows and Mexican cattle. The state will also test all dairy cows in Tulare, Kings, and Fresno counties for the disease. **The announcement came Tuesday during a bovine TB update meeting, when California Department of Food and Agriculture and U.S. Department of Agriculture officials announced that the state's loss of bovine TB-free status is "imminent" after the finding of a second dairy with the disease in one cow.** When it will happen is a matter of how quickly USDA publishes the finding. **The new regulations would require any dairy cow**



**entering California be tested for the disease.** Any state with the bovine TB-free status can freely move animals, but individual states can put requirements on the entry of animals, said Dr. Dorothy York, a state veterinarian and bovine TB expert. **Also, the state would like to restrict cattle from Mexico being grazed in the state to registered pastures, mainly to keep those animals away from pastures that border dairies or cattle operations.**

Source: <http://www.visaliatimesdelta.com/news/stories/20030122/localnews/826709.html>

18. *January 21, Associated Press* — **Chickens, geese destroyed due to bird virus outbreak in Vegas. One turkey and 132 chickens, geese, and ducks have been destroyed by authorities trying to contain an outbreak of a deadly and highly infectious bird virus in a Las Vegas neighborhood. Kimberley Smith, spokeswoman for a multi-agency Exotic Newcastle Disease task force, said Tuesday that nine properties near Nellis Air Force base are believed affected by the avian disease.** Birds have been eradicated and disinfection efforts have begun at six properties, she said. Depopulation teams were due Tuesday to eliminate birds from three more properties. The discovery of infected chickens in a backyard flock last week prompted federal and state officials to expand a strict quarantine on poultry and pet birds from California to southern Nevada, including all of Clark County and parts of Nye County south of Amargosa Valley.

Source: <http://www.rgj.com/news/stories/html/2003/01/21/32544.php?sp1=rgj+News>

19. *January 21, Associated Press* — **Louisiana poultry producers told to watch for Newcastle Disease.** Poultry producers should be on the lookout for a bird disease which forced the quarantine of Southern California's poultry, in case it gets this far, agriculture officials say. **Agriculture Commissioner Bob Odom said Tuesday that he sent a letter and fact sheet about Exotic Newcastle Disease to every poultry producer and veterinarian in Louisiana.** Poultry is Louisiana's largest livestock industry, with a gross farm income of \$493 million and \$474 million worth of processing in the state in 2001.

Source: [http://www.nola.com/newsflash/louisiana/index.ssf?/newsflash/get\\_story.ssf?cgi-free/getstory\\_ssf.cgi?n1480\\_BC\\_LA--PoultryDisease-Lalouisiana](http://www.nola.com/newsflash/louisiana/index.ssf?/newsflash/get_story.ssf?cgi-free/getstory_ssf.cgi?n1480_BC_LA--PoultryDisease-Lalouisiana)

[\[Return to top\]](#)

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

20. *January 21, News Channel 19 (Alabama)* — **Water supply threatened. Authorities say someone has threatened to poison the water supply in Columbus, Mississippi.** Officials say residents are being urged to drink bottled water while state, city, and county authorities investigate the threat. **Columbus officials say there's been no indication the threat is credible. The call was reportedly made about 9 a.m. Tuesday to the Mississippi Emergency Management Agency (MEMA) office in Jackson, Mississippi.** MEMA director, Robert Latham, said the call was from "somebody who said they had gotten a call from another

individual who said he would actually put something in the water." Latham says his office always investigates when such threats are made.

Source: <http://www.whnt19.com/Global/story.asp?S=1093319>

[[Return to top](#)]

## **Public Health Sector**

21. *January 22, Associated Press* — **U.S. to deploy bioterror alert monitors. The government is adapting environmental monitors scattered across the nation to detect bioterrorism, hoping they will provide early warning if smallpox, anthrax, or other deadly germs are released into the air.** The system would retrofit many of the 3,000 existing environmental monitoring stations with new filters to detect biological agents, an administration official said Tuesday. It wasn't clear when, or whether, the administration would officially announce it. Results of the early warnings could be confirmed at a network of laboratories within 24 hours using DNA analysis, the official said, speaking on condition of anonymity.

Source: [http://story.news.yahoo.com/news?tmpl=story2p\\_on\\_go\\_pr\\_wh/bioterrorism\\_detectors](http://story.news.yahoo.com/news?tmpl=story2p_on_go_pr_wh/bioterrorism_detectors)

22. *January 22, Rocky Mountain News* — **Bits of smallpox virus sent to state lab as bioterror test. The Colorado health department's Denver laboratory is one of 23 U.S. labs selected to receive small fragments of the smallpox virus as part of a federal bioterrorism preparedness test. The U.S. Centers for Disease Control and Prevention (CDC) will supply the 23 labs with a new genetic test for smallpox in two or three weeks.** Along with the test, each lab will receive small fragments of genetic material from the smallpox virus, said the CDC's Michael Miller. Later, more smallpox fragments might be sent during "validation exercises" to see if the labs can correctly identify microbe specimens using the new genetic test, said Miller, chief of the laboratory response branch in the CDC's bioterrorism preparedness response program. The tests, called PCR assays, make millions of copies of viral genetic fragments and use them to quickly identify the source organism. "The number of causes of rash illnesses is very, very large, and some of these things could probably be ruled out just by the clinical appearance of the rash," said James L. Beebe, chief microbiologist at the Colorado Department of Public Health and Environment Laboratory. The new smallpox test is also a PCR assay. **The 23 U.S. labs will serve as "beta test sites" to evaluate how well the new assay works. To run the test, each lab will receive smallpox DNA fragments that contain no more than 20 percent of the full genetic sequence, or genome, of the variola virus. Federal officials also want to check the labs' ability to promptly report their findings to the CDC.** "We want to make sure our national reporting system works as well as it did during the anthrax event" of late 2001, Miller said.

Source: [http://www.insidedenver.com/drmn/local/article/0,1299,DRMN\\_15\\_169\\_0415,00.html](http://www.insidedenver.com/drmn/local/article/0,1299,DRMN_15_169_0415,00.html)

23. *January 21, CNN* — **Security to tighten at research labs. Several hundred institutions, from commercial labs to public universities, work with dangerous biological agents, according to the U.S. Centers for Disease Control and Prevention (CDC). Universities and commercial research labs police themselves. The federal government has compiled a list of groups that are restricted from handling the agents, but no agency is charged with enforcing the rules. Nor are background checks required for workers who handle such agents. That will change February 13, when new legislation takes effect and the**

**Department of Justice begins providing a security–risk assessment for anyone with access to restricted biological agents. The assessment will require background checks for scientists or anyone else who can unlock a lab containing such agents.** The government bans numerous groups from working with the biological agents, including foreign nationals from a list of embargoed nations; anyone with a dishonorable discharge from the U.S. military; and anyone who has been committed to a mental facility. The new legislation will increase lab security and add criminal and civil penalties for violations, said Dave Daigle, public relations officer for the CDC. Anyone convicted of possessing or transporting such agents illegally could be fined up to \$250,000 and face up to five years in prison.

Source: <http://www.cnn.com/2003/US/01/20/plague.security/>

[\[Return to top\]](#)

## **Government Sector**

**24. *January 22, CNN* — Senate confirms Ridge as homeland secretary. The Senate voted unanimously Wednesday to confirm Tom Ridge as the first secretary of Homeland Security, a position created in the wake of the September 11, 2001 terrorist attacks.** Ridge, 57, is a former congressman and Pennsylvania governor. President Bush named him as his White House adviser on homeland security after the attacks. In November, Bush nominated him to lead the newly established Department of Homeland Security. "By confirming Tom Ridge, we are taking a big step forward in helping to defend our nation against terrorism," said Sen. Orrin Hatch, R–Utah. "I'm confident that Secretary Ridge will work vigorously to secure our nation and protect Americans and to protect all of us in ways that really have to be undertaken." **The Senate vote was 94–0 to make Ridge the Bush administration's 15th Cabinet secretary. He will lead a department that combines about 180,000 employees from 22 departments and will focus on protecting the country from terrorist attacks. The department will be formally launched Friday, but it's expected to take months before the department becomes fully operational.** Creation of the new department represents the biggest reorganization of the federal government in more than half a century.

Source: <http://www.cnn.com/2003/ALLPOLITICS/01/22/homeland.ridge/index.html>

**25. *January 22, Washington Times* — GSA bars Mexican ID cards.** The General Services Administration (GSA) has suspended recognition of identification cards issued by the Mexican government to its nationals in this country, pending an investigation by the State Department, GSA and other federal agencies. **The "matricula consular cards," used by Mexican nationals to obtain social services and establish bank accounts and used as legal identification for those who have been detained by police, have been issued to hundreds of thousands of Mexican nationals in the United States, including those here illegally.** "The matter of foreign consular identification cards is under discussion both within the State Department and among federal government agencies, including the General Services Administration," the GSA said in a statement made public yesterday. **"While this matter is under deliberation, GSA has suspended the trial acceptance of consular identification cards for admittance to certain federal facilities," the statement said. "GSA will no longer accept consular–issued identification cards as a means of identification, pending further study."** The laminated, digitally coded cards cost \$29, are good for five years and can be obtained from any of the 65 Mexican consular offices in this country by presenting a birth

certificate, an official ID photo and proof of residency, such as a copy of an electricity, water or telephone bill.

Source: <http://www.washingtontimes.com/national/20030122-11837572.htm>

26. *January 22, Washington Post* — **9/11 panel faces time, money pressure.** An independent commission charged with investigating the Sept. 11 terrorist attacks is only beginning to confront a task complicated by a ticking clock, limited finances and the high expectations of those who lost loved ones. **The commission holds its first meeting in Washington on Monday, 16 months after the attacks. It will have just \$3 million and little more than a year to explore the causes of the attacks, preparations for future terrorism and the response to the airline hijackings that killed more than 3,000 Americans at the World Trade Center, the Pentagon and in southwestern Pennsylvania. By comparison, a federal commission created in 1996 got two years and \$5 million to study legalized gambling.** The National Commission on Terrorist Attacks came to life last year in a compromise between Congress and the Bush White House, which had initially opposed it. The 10-member commission, chaired by former New Jersey Gov. Thomas H. Kean, was given 18 months, starting in late November, to get its work done.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A24302-2003Jan21.htm>

27. *January 22, Washington Post* — **Registration amnesty for Pakistanis sought.** Pakistani Foreign Minister Khursid Mahmood Kasuri said today that he would appeal to the Bush administration next week to exempt Pakistani residents of the United States from a program to register thousands of foreign males from more than 20 Muslim countries suspected of harboring terrorists. **The move reflects the growing frustration at home and abroad with a new Justice Department initiative to photograph and fingerprint male citizens of 25 countries, including Iraq, Iran, Syria, Sudan, Libya, Pakistan and Saudi Arabia. The registration program, which requires males from these countries without permanent immigration status and older than 16 to register with the Immigration and Naturalization Service, is part of an effort to better screen foreign visitors to determine if they are linked to terrorist activities.** Kasuri said he would raise the issue along with other matters when he meets Secretary of State Colin L. Powell, national security adviser Condoleezza Rice and members of Congress next week. Kasuri and his advisers said Pakistan would also ask Washington to resume arms sales to Pakistan, lift a travel advisory warning U.S. citizens not to visit Pakistan and increase market access in the United States for Pakistani textiles.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A24784-2003Jan21.htm>

28. *January 21, The White House* — **New White House office coordinates global communications. The Office of Global Communications (OGC) advises on the strategic direction and themes that United States government agencies use to reach foreign audiences.** The Office assists in the development of communications programs that disseminate truthful, accurate, and effective messages about the American people and their government. With State Department Public Diplomacy and Public Affairs remaining at the frontlines of international communications, Global Communications coordinates the work of many agencies and Americans to convey a few simple but powerful messages. These will be aimed to prevent misunderstanding and conflict, build support for and among United States coalition partners, and better inform international audiences. **Lessons learned from the temporary Coalition Information Centers (CIC) have been applied to the new Office. Created to react to our**

adversaries' misinformation, CIC quickly proved that White House–led efforts could facilitate strategic, proactive communications in the war on terror. Last year's focus on the liberation of women in Afghanistan is a prime example. Working closely with the communications office of the Assistant to the President for National Security Affairs, Global Communications recently coordinated communications about the Administration's Ramadan activity and the President's views on Islam.

Source: <http://www.whitehouse.gov/news/releases/2003/01/20030121-4.html>

[\[Return to top\]](#)

## **Emergency Services Sector**

### **29. *January 22, The State (South Carolina)* — Sanford gives SLED chief anti–terrorism role.**

SLED is the state's new lead terrorism response agency and will take on other responsibilities that had been in the Office of Homeland Security, Gov. Mark Sanford said Tuesday. **The State Law Enforcement Division will establish a statewide counterterrorism council to coordinate the roles of police, firefighters and paramedics, Chief Robert Stewart said. SLED also will help devise a plan for spending millions of dollars in federal grants that will help train local emergency responders, Stewart said.** Sanford abolished former Gov. Jim Hodges' Office of Homeland Security when he assigned the new tasks to SLED last Thursday, the day after Sanford was sworn in, said Chris Drummond, Sanford's chief spokesman.

Source: <http://www.thestate.com/mld/state/5002135.htm>

[\[Return to top\]](#)

## **Information and Telecommunications Sector**

### **30. *January 22, CERT/CC* — Vulnerability Note VU#650937: CVS server improperly deallocates memory.** Concurrent Versions System (CVS) is a version control and collaboration system that is widely used by open–source software development projects. CVS is commonly configured to allow public, anonymous, read–only access via the Internet. There is a significant secondary impact in that source code maintained in CVS repositories could be modified to include trojan horses, backdoors, or other malicious code. **The CVS server component contains a "double–free" vulnerability that can be triggered by a set of specially crafted directory requests.** While processing these requests, an error–checking routine may attempt to free() the same memory reference more than once. **Deallocating the already freed memory leads to heap corruption, which an attacker could leverage to execute arbitrary code, alter the logical operation of the CVS server program, or read sensitive information stored in memory.** This vulnerability is resolved in CVS 1.11.5. **CERT recommends the application of a vendor specified patch or upgrade as specified by vendor. Until patches are available and can be applied, consider disabling the CVS server and anonymous access to the CVS server.**

Source: <http://www.kb.cert.org/vuls/id/650937>

31.



*January 22, Microsoft* — **Microsoft Security Bulletin MS03–003: flaw in how Outlook 2002 handles V1 Exchange Server Security Certificates.** There is a flaw in the way Outlook 2002 handles a V1 Exchange Server Security certificate when using it to encrypt HTML e–mail. As a result, **Outlook fails to encrypt the mail correctly and the message will be sent in plain text.** This could cause the information in the e–mail to be exposed when the user believed it to be protected through encryption. S/MIME encryption, which is the most widely used form of e–mail encryption used by Outlook, is not affected. **Microsoft has assigned a risk rating of "Moderate" to this vulnerability. A patch is available at the Microsoft website.**



Source: [http://www.microsoft.com/security/security\\_bulletins/MS03–003.asp](http://www.microsoft.com/security/security_bulletins/MS03–003.asp)

32. *January 22, Microsoft* — **Microsoft Security Bulletin MS03–001: unchecked buffer in Locator service could lead to code execution.** The Microsoft Locator service is a name service that maps logical names to network–specific names. It ships with Windows NT 4.0, Windows 2000, and Windows XP. **A security vulnerability results from an unchecked buffer in the Locator service. By sending a specially–malformed request to the Locator service, an attacker could cause the Locator service to fail, or to run code of the attacker's choice on the system.** The Locator service is not enabled by default on any affected versions of Windows, with the exception of Windows 2000 domain controllers and Windows NT 4.0 domain controllers. **Microsoft has assigned a risk rating of "Critical" for the latter two versions.** A properly–configured firewall would block the calls to the Locator service, which would protect an affected machine from an Internet–based attack. **A patch is available at the Microsoft website.**

Source: <http://www.microsoft.com/technet/security/bulletin/ms03–001.asp>

33. *January 22, Microsoft* — **Microsoft Security Bulletin MS03–002: Cross–Site Scripting flaw in Microsoft Content Management Server 2001.** Microsoft Content Management Server (MCMS) 2001 is an Enterprise Server product that simplifies developing and managing E–Commerce web sites. **A Cross–Site Scripting flaw exists in one of these ASP pages that could allow an attacker to insert script into the data being sent to a MCMS server.** Because the server generates a web page in response to a user request made using this page, it is possible that the script could be embedded within the page that CMS generates and returns to the user, this script would then run when processed by the user's browser. This could result in an attacker being able to access information the user shared with the legitimate site. **An attacker might attempt to exploit this flaw by crafting a malicious link to a valid site that the user intended to visit.** If the attacker were able to get a user to click the link—most likely by sending the link in an email—then **the attacker could alter the data that appeared to be contained on the web pages presented by the legitimate site, monitor the user's session with the legitimate site and copy personal data from the legitimate site to a site under the attacker's control, or access the legitimate site's cookies.** Microsoft has assigned a risk rating of "Moderate" to this flaw. **A patch is available at the Microsoft website.**

Source: <http://www.microsoft.com/technet/security/bulletin/ms03–002.asp>

Current Alert Levels	
 AlertCon: 1 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a>	 Security Focus ThreatCon: 1 out of 4 <a href="http://www.securityfocus.com">www.securityfocus.com</a>
Current Virus and Port Attacks	
<b>Virus:</b>	#1 Virus in the United States: <b>WORM_KLEZ.H</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
<b>Top 10 Target Ports</b>	137 (netbios–ns), 80 (http), 1433 (ms–sql–s), 445 (microsoft–ds), 4662 (???), 139 (netbios–ssn), 53 (domain), 8714 (???), 23 (telnet), 21 (ftp) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center

[[Return to top](#)]

## General Sector

34. *January 22, CNN* — **Al Qaeda terror strategy turns to assassination.** Al Qaeda has been associated with high–profile, explosive terror — September 11, bombings in Pakistan, Kenya, Indonesia and the Philippines — but appears to be turning from mass killings to the assassination of political figures. **Coalition intelligence sources tell CNN that al Qaeda plans to target Western diplomats and other public officials wherever it can.** In late October, U.S. diplomat Laurence Foley was killed outside his Amman, Jordan, home by two men, who were captured and confessed to being members of al Qaeda. Jordanian authorities said the men told them that Foley, a senior administrative officer with the U.S. Agency for International Development, "was not their main target," and that they were planning to kill other Americans in Jordan. **The men trained at al Qaeda camps in Afghanistan, Jordanian authorities said, and received weapons and \$18,000 of a \$50,000 expected payment from al Qaeda chief Osama bin Laden's lieutenant, known as Abu Musa'ab Al–Zarqawi.** Also, CNN has learned that al Qaeda leader Abd Al–Rahim Nashiri — the alleged mastermind of the October 2000 bombing of the USS Cole in Yemen — was planning an assassination campaign before he was arrested in November in the United Arab Emirates. **Another indicator of al Qaeda's strategy is the discovery, earlier this month in a raid on a London flat, of small quantities of the deadly poison ricin — which al Qaeda documents have recommended be used in assassinations.** Senior U.S. officials have told CNN that they believe four men arrested in the raid have ties to Zarqawi.

Source: <http://www.cnn.com/2003/WORLD/asiapcf/central/01/22/alqaeda.assassination/index.html>

[[Return to top](#)]

## **NIPC Products &Contact Information**

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

**NIPC Advisories** – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

**NIPC Alerts** – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

**NIPC Information Bulletins** – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

**NIPC CyberNotes** – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

### **NIPC Daily Open Source Report Contact Information**

Content and Suggestions:	Melissa Conaty (202-324-0354 or <a href="mailto:mconaty@fbi.gov">mconaty@fbi.gov</a> ) Kerry J. Butterfield (202-324-1131 or <a href="mailto:kbutterf@mitre.org">kbutterf@mitre.org</a> )
Distribution Information	NIPC Watch and Warning Unit (202-323-3204 or <a href="mailto:nipc.watch@fbi.gov">nipc.watch@fbi.gov</a> )

### **NIPC Disclaimer**

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.